Forensic Investigation in Digital Environments

Wednesday, 23 October 2019

Dennis Muchiri
Forensics Leader
EY East Africa

Credibility. Professionalism. Accountability

Uphold public interest

Building a better working world

EY
Building a better working world

Contents

ICPAK
Credibility. Professionalism. Accountability

1 **Overview of digital fraud**

2 Cost of cyber related fraud

3 Detecting fraud in a digital environment

4 Digital Forensics in Investigations

5 Prevention in a digital environment

6 Where Forensic Professionals can help

Overview of digital Fraud

1. Overview of digital fraud
2. Cost of cyber related fraud
3. Detecting fraud in a digital environment
4. Digital Forensic in Investigations
5. Prevention in a digital environment
6. Where Forensic Professionals can help

Overview of digital fraud – digital landscape

ICPAK
Credibility. Professionalism. Accountability

Social networking

Wearable computing

Artificial intelligence

Robotics

Drones

Blockchain

IOT

Smart mobility/ On-demand

Predictive analytics

Cloud

3D Printing

Home automation

Cross-industry "blur"

Overview of digital fraud

- ❑ Increased automation; integration of business processes; interconnected supply chains; online presence by organizations in the recent past has led to a shift in fraud arena to cyberspace.
- ❑ Unfortunately, many organizations have not incorporated anti-fraud controls in their systems, and invest in tools and techniques to detect digital fraud.
- ❑ Fraud and other forms of financial crimes have become complicate in the age of cybersecurity

Overview of digital fraud – digital landscape

"…With increased use of ICT there have been increased cases of ICT related frauds in the recent years. Data on fraud reported to Banking Fraud and Investigation Department (BFID) indicates that cases relating to computer, mobile and internet banking are on the rise. Another emerging threat has been cyber-crime where criminals gain unauthorized access to institutions' computer programs and data. ". ~ **CBK Bank Supervision Report 2016**

Overview of digital fraud – digital landscape

ICPAK

Credibility. Professionalism. Accountability

Trends in cybersecurity being exploited to perpetrate fraud

Targeted social attacks using bots

Cyber criminals are getting better at exploiting the ultimate vulnerability – humans. Ever more sophisticated and convincing targeted attacks seek to coax users into compromising themselves.

A fraudster uses a combination of malware, bots, social engineering and other strategies to gain access to a customer's account via digital or mobile channel, requests a new debit card, and uses that card to make purchases.

Digital | Mobile | Card

AI powered attackers

These attacks use AI to make their exploits better and their attacks more intelligent. More attacks are expected on critical financial infrastructure on SWIFT-connected institutions.

A fraudster uses AI technology to (fully) automate practical cybersecurity aspects like exploit generation, attack launch and patch generation processes.

Digital | Mobile | IVR

Downside of encryption

As encryption becomes ubiquitous, it has become much harder for security products to inspect traffic, making it easier for criminals to sneak through undetected.

A fraudster uses purchased or stolen credentials to apply for a credit relationship.

Digital | Mobile | Card

Rising focus on exploits against virtualized and cloud systems

Attacks against physical hardware raise the possibility of dangerous new exploits against virtualized cloud systems.

A fraudster identifies and utilizes vulnerabilities within the digital and mobile channels to gain access to a customer's account.

Digital | Mobile

Overview of digital fraud

Challenges in the management of cybercrime;

- ❑ Inadequate expertise in obtaining & handling digital fraud
- ❑ Evolving nature of e-Crime
- ❑ Lack of employee awareness on the role they should play in identifying fraudulent behaviour (red-flags), reporting and securing digital evidence
- ❑ Ineffective integrity policy framework e.g. lack of updated code of conduct, antifraud policy etc
- ❑ Low prosecution of cyber criminals
- ❑ Low budget allocations for antifraud efforts

Cost of cyber fraud

1 **Overview of digital fraud**

2 Cost of cyber related fraud

3 Detecting fraud in a digital environment

4 Digital Forensics in Investigations

5 Prevention in a digital environment

6 Where Forensic Professionals can help

Cost fraud in a digital environment

- ❑ Communications Authority of Kenya - Cyber threats in Kenya more than doubled in the year to June 2019
- ❑ Kenya National Cybersecurity Centre detected 51.9 million threats for the 2018-2019 period, compared to the 22.1 million in 2017-2018 period
- ❑ Cybercrimes cost in Kenya Sh29.5 bn (2018); Sh21bn (2017); Sh17bn (2016)
- ❑ Cybercrime 'pandemic' may have cost the world $600 billion last year – CSIC & MCAFEE (2018)

Cost fraud in a digital environment

Heavy fines due to regulatory breaches

Negative customer experience/ attrition

Direct and indirect fraud losses

Revenue forgone

Negative customer experience & attrition

Decline in shareholders wealth

Fraud Detection

1 Overview of digital fraud

2 Cost of cyber related fraud

3 Detecting fraud in a digital environment

4 Digital Forensics in Investigations

5 Prevention in a digital environment

6 Where Forensic Professionals can help

Detecting fraud in a digital environment

- ❑Due to sophistication in digital processes in the business environment, it has become increasingly difficult to detect fraud
- ❑Time taken to detect fraud has also increased significantly reducing the value the management derives from responding to delayed detection;
- ❑Volatility of digital evidence - the audit trail for fraudulent activity may also be deliberately not captured or erased making it difficult to determine the culpability

Detecting fraud in a digital environment

- ❑**Cyber Security Operations Centers**
- ❑**Fraud Monitoring Sytems**
- ❑**Data analytics** – Data analysts, auditors, investigators, compliance professionals use of data analytics tools & techniques
- ❑**Internal Audit** – Auditors using systems to monitor transactions in real time or near real time
- ❑**Management reviews**
- ❑**Whistleblowing**

Fraud Investigations

1 **Overview of digital fraud**

2 Cost of cyber related fraud

3 Detecting fraud in a digital environment

4 Digital Forensics in Investigations

5 Prevention in a digital environment

6 Where Forensic Professionals can help

Investigating fraud in a digital environment

❑A fraud examiner should begin with a proposition that the case will end in litigation and this assumption should be maintained throughout the investigation process.

❑All investigations must adhere to the law and no investigation should commence without **predication.**

Investigating fraud in a digital environment

❑Predication refers to the totality of circumstances that would lead reasonable, professionally trained individual to believe that fraud has occurred, is occurring or will occur.

❑In the Kenyan context, the investigation should abide by the provisions of the Constitution 2010, the Evidence Act among other laws.

Investigating fraud in a digital environment

- ❑The rules of collecting electronic evidence are contained in the Evidence Act, Article 78A (Admissibility of Electronic and Digital Evidence)
- ❑Article 78A (1) stipulates that in any legal proceedings, electronic messages and digital material shall be admissible as evidence.
- ❑The act stipulates that in estimating the weight of evidence, the following factors will be considered;

Investigating fraud in a digital environment

❑ the reliability of the manner in which the electronic and digital evidence was generated, stored or communicated;

❑ the reliability of the manner in which the electronic and digital evidence was generated, stored or communicated;

❑ the reliability of the manner in which the integrity of the electronic and digital evidence was maintained;

❑ the manner in which the originator of the electronic and digital evidence was identified

Investigating fraud in a digital environment

- ❑Digital forensics involve recovery and investigation of materials found in digital devices.
- ❑Computer & mobile forensics experts can recover deleted files, temporary autosave files, existing files, data that has been copied moved among others.
- ❑Digital forensics examiners have specialised tools, that are able to extract useful data and evidence that can be adduced in a court of law.
- ❑The volatility of digital evidence calls for due care and a proper chain of custody for integrity.

Investigating fraud in a digital environment

- ❑Digital forensics normally follows the following procedure.
- ❑Planning – Before seizing a digital device, a digital forensics experts should clear all the privacy issues, obtain order where applicable and ensure the equipment is in good condition.
- ❑Seizing – Digital evidence should be seized and stored in a forensically sound way.
- ❑Imaging – At this stage the a forensic image of hard drives and any other media is obtained for analysis.

Investigating fraud in a digital environment

- ❑Processing – The document examiner filters the large amounts of data collected, to remain with relevant information.
- ❑Analysis – specialized software is employed at this stage to identify, extract, collect, examine and store digital evidence. Hardware write blocking software is also crucial in maintaining the integrity of the information at this stage.
- ❑Reporting and testifying – the results of the analysis are fairly and objectively reported.

Investigating fraud in a digital environment

- ❑Acquisition and management of evidence from the seized devices requires high level of skill and availability of the right tools.
- ❑Tools may include;
  - ❑Encase Forensic
  - ❑Forensic toolkit (FTK)
  - ❑ProDiscover Forensics
  - ❑Paraben toolkit
  - ❑Cellebrite UFED
  - ❑Data Analytics Tools

Investigating fraud in a digital environment

Steps to follow with regards to Cyber Response;

- ❑Identify, collect and preserve evidence

  - ❑Acquire all host-based evidence pertinent to the type of incident in a timely & forensically sound way.
  - ❑Identify any running processes, open ports & remote users.
  - ❑Collect network-based log files, including, but not limited to, routers, firewalls, servers and intrusion detection system (IDS) sensors.
  - ❑Conduct necessary internal & external interviews

Investigating fraud in a digital environment

ICPAK
Credibility. Professionalism. Accountability

Steps to follow with regards to Cyber Response...

- ❑Perform forensic analysis and develop fact patterns
  - ❑Conduct a comprehensive forensic examination to determine the attack vector, the scope and depth of the compromise.
  - ❑Identify any unauthorized user accounts or groups, rogue processes and services, and any unauthorized access points.
  - ❑Tell the story of who, what, when, where and how.

Investigating fraud in a digital environment

Steps to follow with regards to Cyber Response...

❑Remove key components of the security incident

- ❑Erase malware and attacker tools.
- ❑Mitigate affected user accounts.
- ❑Uncover the root cause of the breach to determine whether further analysis is required to reveal other vulnerabilities in the network.

Investigating fraud in a digital environment

Steps to follow with regards to Cyber Response…

- ❑Isolate the compromised computers and systems revealed in the analysis

  - ❑Use forensic findings to protect and secure endpoints and the corporate perimeter.
  - ❑Rebuild compromised machines when necessary to provide greater assurance.

Fraud prevention

1 Overview of digital fraud

2 Cost of cyber related fraud

3 Detecting fraud in a digital environment

4 Digital Forensics in Investigations

5 Prevention in a digital environment

6 Where Forensic Professionals can help

Preventing fraud in a digital environment

- ❑In digital environment, an effective method to prevent or deter must "create a perception of detection" for all the organizational actors.
- ❑Some of the techniques used to prevent fraud and malpractices include;
  - ❑Conducting regular fraud prevention check ups
  - ❑Establishing fraud risk oversight and ownership at board and management levels respectively.
  - ❑Establishing and implementing antifraud policy and code of conduct.

Preventing fraud in a digital environment

- ❑Fraud training on employees and 3rd parties
- ❑Proactive data analysis and monitoring
- ❑Job rotation and mandatory vocations for all staff members.
- ❑Recognition of whistleblowers
- ❑Surprise audits

Forensic Professionals

1 **Overview of digital fraud**

2 Cost of cyber related fraud

3 Detecting fraud in a digital environment

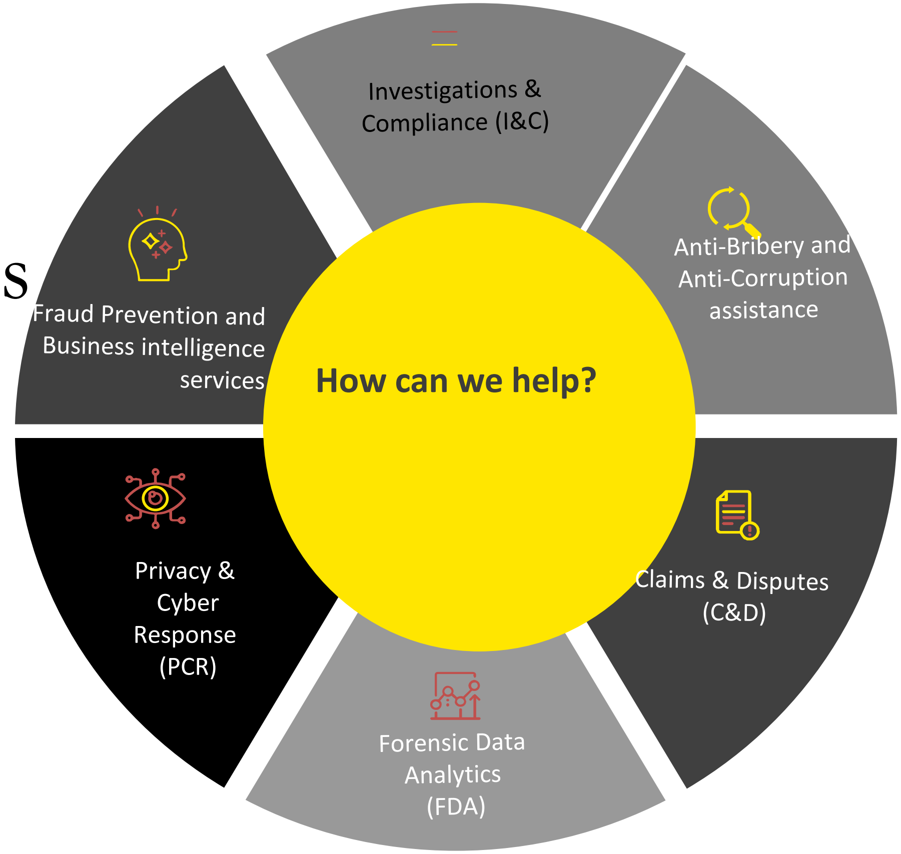
4 Digital Forensics in Investigations

5 Prevention in a digital environment

6 **Where Forensic Professionals can help**

Forensic and Integrity Services

- ❑ Investigations and compliance
- ❑ Computer forensic services and discovery
- ❑ Anti-Bribery and Anti-Corruption assistance
- ❑ Claims and disputes
- ❑ Forensic Data Analytics
- ❑ Privacy & Cyber Response


How can we help?
Investigations & Compliance (I&C)
Anti-Bribery and Anti-Corruption assistance
Claims & Disputes (C&D)
Forensic Data Analytics (FDA)
Privacy & Cyber Response (PCR)
Fraud Prevention and Business intelligence services

Investigations and compliance

- ❑ This focus on the following
  - ❑ Allegation identification
  - ❑ Allegation confirmation
  - ❑ Evidence gathering
  - ❑ Reporting
  - ❑ Disciplinary action
  - ❑ Criminal Prosecution

Forensic Data Analytics

- ❑Analysis of large volumes of electronic data
- ❑Identification of additional evidence/ Relationship/ behaviour patterns/ suspects.
- ❑Link factual findings to case
- ❑Early case assessment

Computer Forensic services & Discovery

- Discovery services help answer “who, what, where, when and how" questions.
- We do forensic image acquisition of electronic stored information from various digital media and devices.
- Forensic analysis of acquired electronic stored information by means of keyword search analysis.
- Recovery of deleted information
- Extraction of user created data.

Privacy & Cyber Response

- We help in Identifying and addressing vulnerabilities in the IT environment
- Developing an effective Cyber Breach Response Management (CBRM) Plan
- Help determine how and when the system compromise occurred, provide factual findings on who may have been responsible and what the impact was to the organization
- Preparing robust evidence for use in any criminal proceedings that may follow

Anti-Bribery and Anti-Corruption assistance

- □We help with the following;
  - □Corruption risk and compliance assessment
  - □Corruption awareness training
  - □Development and implementation of effective Ant-Corruption Programmes
  - □Pre-appointment and corruption due diligence reviews
  - □Investigations

Claims and disputes

- ❑Fact finding and discovery, analyses and/or damages quantification in disputes relating to;
  - ❑Financial transactions
  - ❑Construction/insurance companies
  - ❑Purchase price/purchase transactions disputes
  - ❑Anti-trust/competition matters
  - ❑Regulatory based claims
  - ❑Breach of contract claims
  - ❑Accounting malpractice.

Fraud prevention and business intelligence services

- ❑**Fraud prevention services**
  - ❑Develop a holistic fraud risk management strategy including fraud risk assessment training.
  - ❑Conduct forensic maturity survey to understand the current and desired states of the fraud prevention and detection initiatives.
  - ❑Benchmarking fraud related policies and procedures to leading practice.

Fraud prevention and business intelligence services

- ❑ **Business intelligence services**
  - ❑ Business track records, corporate interests and possible adverse data
  - ❑ Asset tracing
  - ❑ Client acceptance
  - ❑ Conflict of interest and undisclosed business affiliations
  - ❑ Director and principal business checks
  - ❑ Criminal and qualification checks
  - ❑ Third party due diligence

Questions & Answers

ICPAK
Credibility. Professionalism. Accountability

Thank you

Dennis Muchiri
Forensics Leader
EY East Africa
dennis.muchiri@ke.ey.com